```
 d his
     (FILE 'USPAT' ENTERED AT 16:23:49 ON 18 OCT 96)
L1             0 S VIRU? AND PROXY SERVER
L2             2 S PROXY SERVER
L3             0 S L2 AND VIRUS
L4             4 S SERVER (P) SCAN? AND VIRUS?
L5             0 S L4 AND DAEMON
L6             0 S DAEMON AND VIRUS AND SERVER (P) SCAN?
L7             0 S VIRUS AND ENCODED (P) PROTION (P) MAIL
L8             0 S DETECT? (P) VIRUS  AND MAIL MESSAGES, SCANN?
L9             6 S VIRUS (P) MAIL
L10            1 S SMTP AND VIRUS
=> s l10 and daemon
            91 DAEMON
L11           0 L10 AND DAEMON
=> s l10 and encoded
         36822 ENCODED
L12           0 L10 AND ENCODED
=
```

US PAT NO: 5,511,163 [IMAGE AVAILABLE] L4: 3 of 4
TITLE: Network adaptor connected to a computer for **virus** signature recognition in all files on a network

ABSTRACT:

A . . . adaptor can perform an assembling and scanning of substantially all files on the network and carry out a recognition of **virus** signatures. The individual file packets circulation in the network are assembled, said file packets being assembled in a file and scanned for **virus** signatures. When a **virus** signature is detected in the file, information is simultaneously provided on the transmitting stations and the receiving stations, whereafter it. . .

SUMMARY:

BSUM(5)

A ring network can be connected to a network **server**. The network **server** can comprise a network program accessible for the users at each work station. Each user can furthermore have access to the logic drive of the network **server**, whereby the user can enter programs and data which can subsequently be read by another user without floppy disks being exchanged between the users. The network **server** can furthermore include a **virus** program accessible for the user of a work station so as to enable him to **scan** the local disk for virae. The user can carry out a **virus** **scanning** at regular intervals. A **virus**, if any, may, however, have infected a large number of work stations before being detected.

SUMMARY:

BSUM(7)

The object of the invention is to provide a data processing system of the above type, whereby a **virus**, if any, and computers infected thereby are detected far quicker than previously so as to limit the spreading of the **virus**.

SUMMARY:

BSUM(8)

The . . . which together with the adaptor can catch and scan all files on the network and carry out a recognition of **virus** signatures (bit patterns), if any, in the files. As a result, the file packets circulating in the ring network are. . . one file. After the assembling in one file, the packets are scanned for detection of virae, if any. If a **virus** signature is detected in the file, information on the transmitting and receiving stations is provided and an alarm is activated, whereby a further spreading of the **virus** can be prevented.

SUMMARY:

BSUM(9)

Moreover . . . computer connected to the adaptor may be adapted to transmit a so-called "vaccine" to the computers optionally infected by said **virus** or said virae. The close-down period of the system due to detection of a **virus** has thereby been reduced to zero.

SUMMARY:

BSUM(10)

Furthermore . . . to start a scanning on the infected computers by means of a program known per se, said program neutralizing the **virus**.

SUMMARY:

BSUM(11)

In . . . data on the local network and to actuate an alarm if an unusual interchange of data, such as an unknown **virus** signature, is recognized. In this manner it is also possible to detect hitherto unknown virae and thereby to obtain a better **virus** detection than previously known.

DETDESC:

DETD(2)

The . . . computers 2 in form of personal computers interconnected through a local network in form of a ring network 1. A **virus** can infect a personal computer 2 via a floppy disk 3 inserted in the computer 2 copying the program on the floppy disk 3. As a result the computer is infected by the **virus** in said program. The infected program can then be transferred via the network to one or several of the remaining personal computers 2 connected to the network 1. The **virus** is transferred when the program or the program file is divided into packets being transmitted in series via the ring. . .

DETDESC:

DETD(3)

The network 1 is furthermore connected to a network **server** 5. Previously, the network **server** 5 included a program allowing the user to perform a **virus** **scanning** at regular intervals of the programs in the personal computer 2. Such a **virus** control is, however, encumbered with the drawback that a **virus**, if any, may be spread to a large number of work stations of the data processing system before an alarm. . .

DETDESC:

DETD(4)

According . . . logic in the network adaptor 7 assembles the packets in files, cf. FIG. 3, for a scanning and detection of **virus** signatures, if any. The adaptor 7 has been symbolized in FIG. 1 by means of a magnifying glass and is connected to the computer 8. The computer 8 is able to scan the files and recognize **virus** signatures, if any.

DETDESC:

DETD(5)

A . . . program signatures in order to ensure that said program signature is in fact a portion of the complete program. A **virus** is in fact a program and can therefore be recognized in the same manner. As far as a known **virus** is concerned all the files of an electronic data processing system can be scanned for the signature of said **virus** by the system performing a comparison with said signature. If the signature is a portion of a file, said file may have been infected. A large number of programs are able to scan for known **virus** signatures. These programs render it possible to determine whether an electronic data processing system is infected by known virae.

DETDESC:

DETD(6)

When a **virus** is detected, an alarm is instantaneously activated and a so-called "vaccine" is transmitted to the personal computers having received infected. . . instance by means of the program "Clean" sold by the company Mcafee. This program can erase or write over a **virus** program typically placed in front of or after the actual program. If the **virus** program is placed in front of the actual program, an indication can be provided after the erasing of or writing over said **virus** that the actual program does not start until later. A quick transmission of such a vaccine minimizes the spreading of the **virus**. The principle is particularly suited in connection with a ring network as the information packets pass the adaptor 7 during. . .

DETDESC:

DETD(8)

The data processing system can be further developed so as also to be able to recognize a new **virus** and send a vaccine to it. The further development is found in the fact that the work station 8 or. . . in case of an abnormal interchange of data in form of an unknown signature possibly corresponding to yet another unknown **virus**.

DETDESC:

DETD(14)

A perceptron comprising one of more neurons can be used for recognizing a pattern, such as a **virus** signature. A perceptron for recognizing a **virus** signature includes preferably at least two neurons. It is assumed that a **virus** signature has a maximum length of m hexadecimal figures of 8 bits. A hexadecimal figure of 8 bits can assume 256 various values. The input signal vector X must then have the dimension m.multidot.(256+1). All possible combinations of **virus** signatures therefore result in various X-vectors.

DETDESC:

DETD(20)

Then the perceptron is presented to a large number of **virus** signatures as well as to a large number of signatures without **virus**.

DETDESC:

DETD(21)

When the signature is a **virus**, the class for the neuron 1 must be 1, whereas the class for neuron 2 must be 0. When the signature is not a **virus**, the class for neuron 1 must be 0 whereas the class for neuron 2 must be 1, i.e.:

DETDESC:

DETD(22)

The signature is a **virus** :Neuron 1.Y=1 and Neuron 2.Y=0.

DETDESC:

DETD(23)

The signature is not a **virus** :Neuron 1.Y=0 and Neuron 2.Y=1

DETDESC:

DETD(24)

After the supply of a **virus** signature, the weight factors of the neurons must be adjusted by means of the programming instructions until the perceptron has. . .

DETDESC:

DETD(26)

A new **virus** often resembles a known **virus** as many new virae are developed on the basis of known virae. A few virae are furthermore able to change the signature all the time by adding NOP's (no operation) to the signature. In other words the **virus** mutates. An NOP does not involve activity, and the functions of the **virus** remain unchanged. The signature of the **virus** is, however, changed. In many cases the perceptron is also able to recognize such routants as the insertion of NOP's. . .

CLAIMS:

CLMS(1)

We . . .

can perform an assembling and scanning of substantially all files on the network (1) and carry out a recognition of **virus** signatures, if any, in the files, the computer (8) being adapted to provide information on the place of origin of. . . of data on the local network (1) and for activating an alarm if an unusual interchange of data resembling a **virus**, such as an unknown **virus** signature, is recognized.

CLAIMS:

CLMS(2)

2. . . . processing system as claimed in claim 1, which includes

computer means (2) connected to the adaptor (7) for transmitting a **virus** to the computers (8) optionally infected by said **virus**.

=

```
 d ti ab

**06-350784**                                              L10: 1 of 1

TITLE:  FACSIMILE EQUIPMENT


ABSTRACT:

 PURPOSE: To provide a facsimile equipment in which the infection of a
computer virus can be suppressed.

 CONSTITUTION: When a file transmitting request is accepted from other
personal computers PC1, PC2,..., PCm through a local network, when a
floppy disk is mounted on a floppy disk device, and a file is received
from the other terminal, whether or not an accepted file, file preserved
in the floppy disk, and received file are infected with the computer
virus is checked. When they are infected with the computer virus, the
file is deleted, or a user is allowed to be informed of the result, so
that a situation that the computer virus spreads in the local area
network can be sharply suppressed.

 COPYRIGHT: (C)1994,JPO
=> d cit

1.  **06-350784**, Dec. 22, 1994, FACSIMILE EQUIPMENT; FUTOSHI OSETO,
H04N 1/00; G06F 11/00
=
```